

---

# *Joint Information Operations in Counterinsurgency Warfare*

## *Part II*

by Major Norberto Menendez

**Editorial Abstract:** In this academic paper Major Menendez examines some of the classic definitional and authority issues related to Information Operations planning an execution as applied to counter insurgency warfare.

In the journal article by Major Lane Packwood USA titled “Joint IO in Counterinsurgency Warfare: A Critical Gap in Capability”, the author highlights a clear gap in the capability of the military to target the support of the “neutral or passive majority”<sup>1</sup> by information operations (IO) core capabilities, supporting capabilities, and related capabilities. Potential solutions offered try to draw lines between Public Affairs (PA), Psychological Operations (PSYOP), and the new potential capability named defense support to public diplomacy. We clearly have a gap in capability, but I would contend that to fill this gap, we do not need to “split hairs” between the duties and responsibilities of PA and PSYOP communities. The answer to the gap in

capability has more to do with the ability of operators (S3s, G3s, J3s, N3s, etc) to synchronize the effects they are trying to achieve, and their ability to have PA and PSYOP deliver this message to their respective audiences.

IO by definition “seeks to influence the behavior of selected target audiences and decision makers through the use of information and information systems. Conversely, defensive IO seeks to shield or defend friendly decision-makers or audiences from being unduly influenced by an adversary’s use of information or information systems.”<sup>2</sup> To this end, in the counterinsurgency fight, our focus shifts the “neutral majority” whose support is needed to win the conflict. In others words, in addition to a kinetic fight against insurgents and terrorists, we are also engaged in a non-kinetic fight for the hearts and minds of the people. In the context of the Global War on Terrorism (GWOT), this happens through engagements (including a visit from the President of the United States to



US Soldier Aids Afgan Child  
Source: defenseimagery.mil

the Iraqi President or Afghan President, to a squad leader interacting with an Iraqi or Afghan family while on patrol) the important point to understand is that this happens in the Information Domain. Every action and counter-action on the battlefield, whether it is a firefight or a humanitarian mission, will eventually move into the information domain where it will be dissected and examined by all, most often through the filter of the person entering the information into the domain. This is where we need the most agility and flexibility, and where PSYOP and PA can complement each other and work together within the scope of their mission to gain information dominance.

Further defining how the two capabilities should be synchronized, let us examine the respective missions. PSYOP's mission is to influence the behavior of foreign target audiences by conveying selected information to influence emotions, motives, objective reasoning, and ultimately the behavior of a foreign audience.<sup>3</sup> By its very nature, PSYOP seek to present information or spin information in a way that supports the United States' national interests. On the other hand, PA's mission is to "fulfill the Army's obligation to keep the American people and the Army informed, and helps to establish the conditions that lead to confidence in America's Army and its readiness to conduct operations in peacetime, conflict, and war."<sup>4</sup> Unlike PSYOP, PA serves as a transfer point for information both in and out of the theater of operations. PA's role with misinformation or propaganda is reactive vs. PSYOP, which is proactive. When done properly both organizations play a critical role within the information domain, and their employment is more an issue of synchronization rather than authorities and expertise.

To explain this, consider the Afghan counter-insurgency approach published by a Combined Joint Task Force in 2007. The framework is built around two pillars: the first seeks to build Afghan capacity through five objectives; the second seeks to degrade destabilizing forces through four objectives. The



**ANA Soldier and Afghan Police Officer Receive Mine Clearing Training from a US Soldier**  
Source: defenseimagry.mil

objective is to strengthen the Afghan nation by replacing fear and uncertainty with trust and confidence on Afghan leadership and institutions. There must be a specified strategy, with the many implied tasks requiring coordination and synchronization inside the information domain to achieve the stated objective.

As operations officers develop a plan to implement this strategy, they must understand that execution of the plan and especially the effects of the plan will ultimately be judged within the information domain. PA, as the hub of information in and out of the headquarters, must understand that their



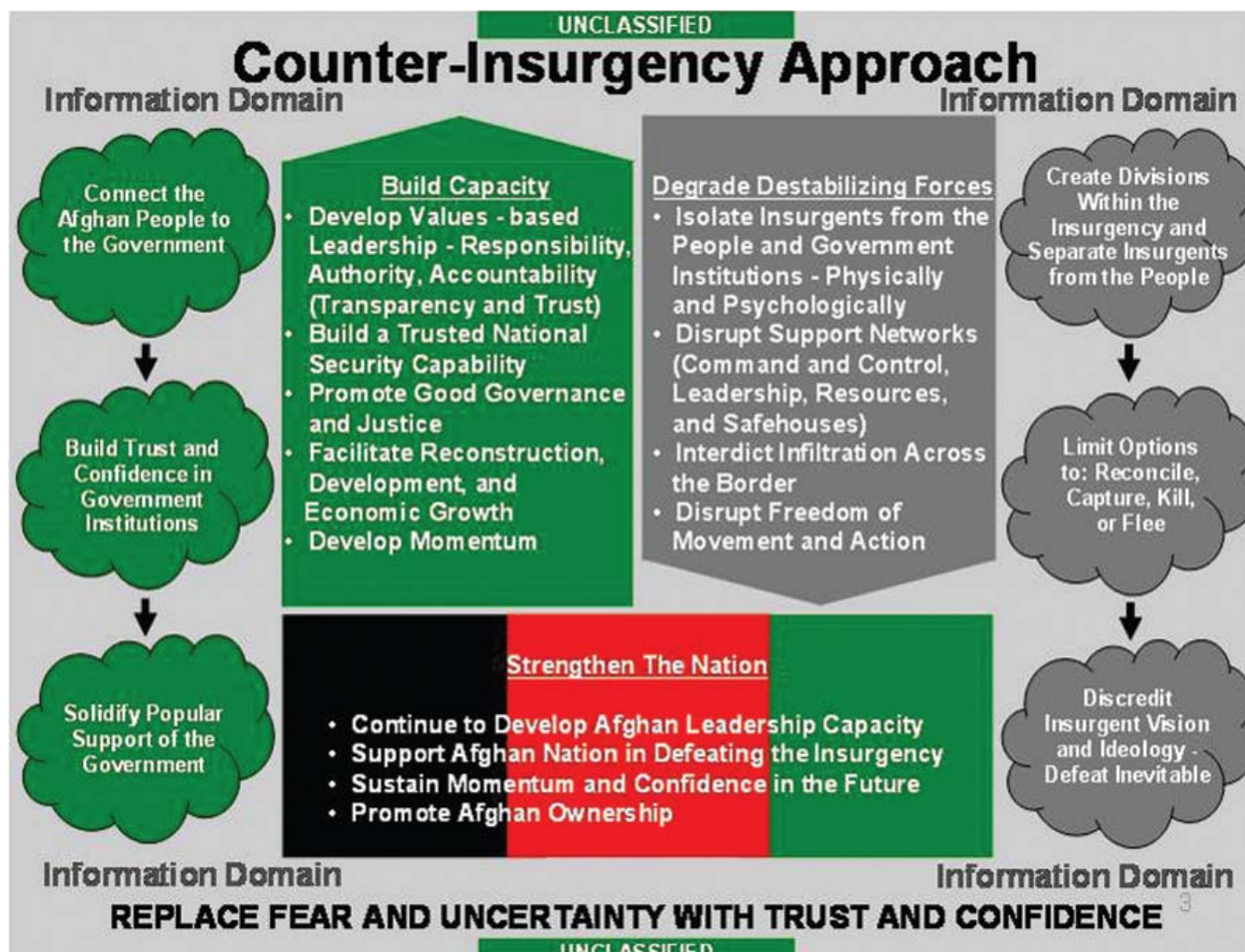
actions and sometimes lack of actions ultimately have some sort of reaction or influence within the Global Information Environment (GIE). In the age of instant communications, PA officers must understand that even though their mission calls for them to inform the American public and the Army, the GIE will ensure that information intended for American audiences will be read and scrutinized by people all over the world. Even though their potential audience has increased significantly, PA principles to deliver information and not propaganda still stand and should not be altered. However, they must be cognizant of how the information they are delivering might be utilized by the enemy and be prepared to counter it; therefore, changing the reactive nature of public affairs to proactive.

PSYOP within the information domain are a little easier to delineate. In the case of this strategy, PSYOP is engaged in discrediting the enemy and influencing the people of Afghanistan to support the elected government. They are focused on target audiences and the delivery of a message that supports the stated strategic vision. PSYOP is very proactive in nature, but has little reactive capability when unplanned events introduce themselves.

Within the information domain, stories, data, and pictures act as soldiers, airplanes, and bombs do in the operational domain. Consider this analogy: Artillerymen are normally obsessed with shooting long-range weapons (affected by a number of external influences such as air, pressure, projectile imperfection) with incredible

precision. Anything short of hitting a target regardless of the range (almost impossible without the aid of "smart" rounds) is a failure. However, they often fail to recognize that even though the round did not impact on someone's forehead, whatever that enemy was doing at the time the round exploded, he is no longer doing. In other words, that lack of lethality does not change the fact that the enemy is no longer walking in the open, digging, or sleeping. The fact that the round exploded nearby has caused the enemy to change his behavior. Information works much in the same way. Introducing a piece of information into an operation will cause the enemy to do something different. In the case of this strategy, this information will often be the "neutral majorities" catalyst to begin supporting the government

## Counter Insurgency Methodology and Strategy



or the insurgents. Whether the information is delivered by PSYOP, or delivered as part of the PA information strategy, the information will cause a reaction and the need for planning and synchronization, as opposed to, new missions, parameters, and organizations. The later is often an unneeded result.

IO officers, as the synchronizers of capabilities, are the ones responsible for the synchronization of PSYOP and PA in the Counter Insurgency (COIN) operation. This fills the identified gap in capability. The strategy creates a clear vision of what the objective is and how it is to be achieved, and the operational plan synchronizes all the capabilities to achieve the objectives. PSYOP and PA personnel work together to deliver one message. One by influencing (PSYOP) and one by informing (PA); however, if information or the act of informing will cause the enemy or the “neutral majority” to do something different, then information or the act of informing will have a reaction. So, both have some degree of an influencing effect. Therefore, the information produced for dissemination in PA channels could potentially have the same level of influence as the information produced by PSYOP.

In practice, operation officers close the gap by identifying the objectives for an operation and identifying the information they plan to use to influence multiple audiences as part of their intelligence preparation of the battlespace (IPB). These then become PSYOP tasks within the operation. Then the next step is to assess what information is coming out of the operation that the enemy might use to influence friendly forces (NATO, Afghan government, Afghan people, etc.) in a negative or inaccurate way as a form of propaganda, and begin to plan how to counter that propaganda. These become PA tasks within the operation. This is where the perceived gap between PSYOP and PA occurs. PSYOP planning at this point is adversarial focused, as it should be, and does not focus on countering propaganda. However, PA is charged with countering propaganda by its own doctrine. PA planners involved in the operation can begin to develop enemy likely courses of action based on an assessment of previous operations, and then begin to “war-game” potential stories the enemy might use to their advantage. They also must develop plans and strategies on how to counter those possible stories. PA is not being tasked to influence by propagandizing or creating false stories, PA is tasked to prepare truthful




**ANA and Coalition Forces Conduct Night Operations**  
Source: [defenseimagry.mil](http://defenseimagry.mil)



statements based on the most accurate and up to date information available and to expeditiously release the information to counter enemy propaganda. This is the same as identifying a tactical risk and mitigating it through the introduction of a capability or resource in the operations. In other words, a risk has been identified in the information domain, and there is a plan to mitigate that risk. Operators synchronizing PA efforts for the operation are simply using their capability to deliver the truth in the Counter Insurgency (COIN) fight.

In conclusion, rather than reforming PA or PSYOP to fill a perceived gap in capability in the joint IO COIN warfare, we should be looking at training IO officers to identify threats, audiences, messages, and capabilities within the information domain. The relationship between PA and PSYOP is complementary instead of adversarial or simply non-complementary. In a COIN environment where the enemy is not bound by any journalistic code of

ethics, and where news outlets do not require enemy messages to be truthful in an effort to deliver shock value and ratings, it is important to be fast with the truth, whatever that might be. The old news industry adage “if it bleeds, it leads and reads” is still very valid today. In the age of instant communications and sensory overload, people will often catch the first headline published for a story, remember it or create a perception of it, therefore being influenced, and move on to the next story. People will almost never read a retraction or clarification of a story. It is for this reason that proactive and agile PA posture is critical to all operations. As soon as the enemy delivers a story that seeks to influence the “neutral majority” with inaccuracies and misinformation, PA must be ready to counter that story with the most truthful information available. In the fight for the hearts and minds of many, to include support of NATO partners in the Afghan case or congressional and public opinion in the United States, we must be ready to present the truth accurately and swiftly.

It is for these reasons, that operations officers must synchronize PSYOP and PA messages and have a running staff estimate of how the enemy might use information to their advantage. The answer is not within the capabilities, it is within the synchronization of those capabilities in support of the commander’s operational plan. 

---

**Editor’s Note:** This paper by Major Menedez was first published as part of the academic requirements for the United States Naval War College. His views on IO Synchronization are important to consider and are a common thread in IO planning and execution. There are lessons to be learned in all of these contributions and submissions. At IO Sphere we appreciate them all.

---

### **Footnotes:**

1. *FM 3-24 page 6-15*
2. *Information Operations (elective manual) page 1*
3. *FM 3-05-30 page 1-2*
4. *FM 46-1 page 3.1*



US Marines During Platoon Briefing in Iraq  
Source: defenseimagry.mil